BackTrack Security Guide

Contents

BackTrack Security Guide

Your Data, Your Control

BackTrack is built with your privacy and data security as top priorities. This guide explains what you need to know to keep your practice data safe.

□ Database Encryption

What It Means

All patient/client data is encrypted using military-grade encryption. Your database password is the only key that can unlock your data.

What You Should Do

1. **Choose a Strong Database Password**
   - Use at least 12 characters
   - Mix uppercase, lowercase, numbers, and symbols
   - Don't use common words or personal information
   - Example: `Pr@ct1ce!SecureDB#2026`
2. **Store Your Password Safely**
   - Write it down and keep it in a safe place
   - Use a password manager (LastPass, 1Password, Bitwarden)
   - **Never share it via email or text**
3. **Keep Your Password and Recovery Methods Safe**
   - Your database password encrypts all your data
   - Your Support Code OR TOTP authenticator allows password recovery if needed
   - Keep them in separate secure locations
   - Write them down (support code) and store in a safe or password manager
   - Consider setting up TOTP for an additional recovery option

Support Code & TOTP (Emergency Recovery)

When you first set up BackTrack, you receive a **Support Code** and can optionally set up **TOTP authentication** (Google Authenticator, etc.) for support access.

Two Ways We Can Help You Recover: 1. **Support Code** - A unique text string shown during initial setup 2. **TOTP/Authenticator App** - If you've configured it, we can verify your identity using your authenticator app

What they do: - Allow our support team to verify your identity as the legitimate database owner - Enable us to help you reset your database password if you forget it - Provide multiple recovery paths for better protection

Critical: If you lose your database password AND don't have either recovery method (support code OR TOTP), AND you don't have a backup, your data cannot be recovered. This is by design for security—no backdoors means no one (including us) can access your data without proper authorization.

□ Secure Image & Signature Storage (BLOB Storage)

What It Means

BackTrack stores sensitive images (profile photos and doctor signatures) directly in your encrypted database, not as files on your hard drive. This is called "BLOB storage" (Binary Large Object).

Why This Matters

Security Benefits: - □ **Automatic Encryption** - Images are encrypted with your database password - □ **Prevents Misuse** - Signature files can't be copied or extracted for forgery - □ **Automatic Sync** - Images sync across all your computers automatically - □ **No Loose Files** - Nothing sensitive stored in accessible folders - □ **EXIF Privacy** - Photo metadata (location, camera model) is stripped automatically

What's Protected

- **Profile Photos** - Staff and provider profile images
- **Doctor Signatures** - Electronic signatures for prescriptions and certificates
- **All encrypted** within your database

What You Should Know

1. **QR Code Uploads** - Photos taken with your phone are automatically rotated correctly
2. **Sync Automatically** - Upload once, available on all your computers
3. **Backup Included** - Images are part of your regular database backups
4. **No Migration Needed** - Old image files remain until you re-upload (no data loss)

□ User Account Security

Strong Passwords

Each user should have their own account with a strong password: - At least 8 characters (longer is better) - Mix of letters, numbers, and symbols - Different from any other password they use - Changed every 90 days (recommended)

User Roles

- **Admin** - Full access, can manage users and settings
- **Doctor** - Clinical access, can see all patient data

- **Staff** - Limited access, can schedule and check-in patients

Best Practice: Only give users the access level they need for their job.

□ Two-Factor Authentication (MFA)

What Is It?

MFA adds a second layer of security. Even if someone steals your password, they can't log in without your phone.

How to Enable It

1. Go to **Settings** □ **User Management**
2. Select your user account
3. Click **Enable MFA**
4. Scan the QR code with an authenticator app
5. Save your backup codes in a safe place

Recommended Authenticator Apps (All Free)

- **Google Authenticator** (iOS, Android)
- **Microsoft Authenticator** (iOS, Android)
- **Authy** (iOS, Android, Desktop)
- **FreeOTP** (iOS, Android)

Backup Codes

You receive 10 one-time backup codes when you enable MFA. Keep these safe! You'll need them if you lose your phone.

□ Backup Your Data

Why Backups Matter

Hard drives fail. Computers get stolen. Accidents happen. Regular backups ensure you never lose patient data.

How to Backup

1. Go to **Settings** □ **Database Backup**
2. Click **Create Backup**
3. Save to an external drive or cloud storage
4. **Test your backups** - restore them to make sure they work

Backup Schedule (Recommended)

- **Daily** - If you see lots of patients
- **Weekly** - For smaller practices
- **Before major updates** - Always backup before upgrading

Where to Store Backups

Good: - External USB drive (kept in a safe) - Encrypted cloud storage (Dropbox, Google Drive with encryption) - Second computer in a different location

Bad: - Same computer as your main database (defeats the purpose) - Unencrypted cloud storage - USB drive left in the office where it could be stolen

---

Network Security

Multi-Computer Sync

If you use BackTrack on multiple computers, they sync over your local network. This is secure, but follow these practices:

1. **Use a Secure Wi-Fi Network**
   - Strong WPA3 or WPA2 password
   - Not the same password as your database
2. **Firewall Rules**
   - BackTrack uses ports 8765-8766
   - Only allow these ports on your local network
   - Don't expose them to the internet
3. **Keep Computers Updated**
   - Install operating system security updates
   - Keep antivirus software current

Web Check-In & Patient Onboarding

QR Codes and Links

When patients use web check-in or complete onboarding, they access a temporary link. These links: - Expire after use - Are unique to each patient - Don't expose any patient data

SMS Reminders

If you send SMS reminders, patient phone numbers are not stored by third parties. Messages are sent via email-to-SMS gateways.

Physical Security

Technology is only part of security. Protect your physical workspace:

1. **Lock Your Computer**
   - When you step away, always lock your screen
   - Windows: `Windows Key + L`
   - Mac: `Command + Control + Q`
   - Linux: `Super + L` or `Ctrl + Alt + L`
2. **Don't Share Logins**
   - Each person should have their own account
   - Sharing accounts makes auditing impossible
3. **Secure Your Office**
   - Keep computers in locked rooms after hours
   - Don't leave patient data visible on screens
   - Shred printed patient information
4. **Protect Your Devices**
   - Enable full-disk encryption on your computer
     - **Windows:** BitLocker
     - **Mac:** FileVault
     - **Linux:** LUKS (enable during OS installation)
   - Use a strong login password
   - Enable "Find My Device" features

What To Do If Something Goes Wrong

Lost or Stolen Computer

1. **If enabled:** Use remote wipe (Find My Device)
2. Change all user passwords immediately
3. Review audit logs for suspicious activity
4. Contact law enforcement
5. Restore your database on a new computer from backup

Suspicious Activity

If you suspect unauthorized access: 1. Change all passwords immediately 2. Review the **Audit Log** (Settings Audit Log) 3. Disable any suspicious user accounts 4. Contact support if you need help

Forgot Database Password

If you have your Support Code OR TOTP authenticator: 1. Contact support 2. Provide your support code OR use your authenticator app to verify your identity 3. We can help you reset your database password 4. Your data remains safe and accessible

If you don't have either recovery method: - **AND you have a recent backup:** Restore from backup on a new installation - **AND you don't have a backup:** There is no way to recover your

data

This is why four things are critical: 1. Keep your Support Code in a safe place (separate from your database password) 2. Consider setting up TOTP authenticator for an additional recovery option 3. Make regular backups 4. Store at least one backup in a different physical location

---

□ Security Checklist

Use this checklist to ensure your practice is secure:

- ☐ Strong database password (12+ characters)
- ☐ Database password stored safely (password manager or safe)
- ☐ Support code saved in secure location
- ☐ TOTP authenticator configured for support access (optional but recommended)
- ☐ Each user has their own account with a strong password
- ☐ MFA enabled for all admin users (at minimum)
- ☐ Backup codes for MFA saved securely
- ☐ Regular backups (weekly or daily)
- ☐ Backups stored in safe, separate location
- ☐ Backup restore tested at least once
- ☐ Full-disk encryption enabled on all computers
- ☐ Wi-Fi network secured with WPA2/WPA3
- ☐ Computers lock automatically after 5 minutes of inactivity
- ☐ Operating system and antivirus kept up-to-date
- ☐ Users trained to lock their screens when away
- ☐ Audit log reviewed monthly for suspicious activity

□ Need Help?

If you have questions about security or need assistance: - **Email:** support@krankybearbacktrack.com - **Documentation:** See README.md and TROUBLESHOOTING.md - **Emergency:** If you suspect a security breach, contact us immediately

---

Remember

Security is a shared responsibility. We've built BackTrack to be secure by design, but your practices—strong passwords, regular backups, physical security, and keeping your recovery methods safe—are equally important.

You're never alone: If you forget your database password, we can help you recover it using your Support Code OR your TOTP authenticator (if configured). If you lose all recovery methods, backups are your last line of defense.

Together, we keep your patients'/clients' data safe.